AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

HARDENING UNMANNED AERIAL SYSTEMS AGAINST HIGH POWER MICROWAVE THREATS IN SUPPORT OF FORWARD OPERATIONS

by

Coningsby J. Burdon, Maj, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements for the Degree of

MASTER OF OPERATIONAL ARTS AND SCIENCES

Advisor: Dr. John P. Geis II

April, 2017

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

About the Author

Major C.J. Burdon is assigned to the Air Command and Staff College, Air University, Maxwell Air Force Base, Alabama. He is a US Air Force C-17A Globemaster III evaluator pilot, highly-experienced in aircrew training processes, as well as the employment of air-land, airdrop, and Special Operations airlift. Most recently, Major Burdon was assigned to Altus Air Force Base as a C-17 Formal Training Unit Evaluator Pilot and Chief of the 97th Air Mobility Wing Commander's Action Group. Major Burdon has previously held positions at Joint Base Charleston's 437th Airlift Wing as the Special Operations DO, Process Improvement Chief, and squadron Tactics Officer. He has deployed four times in support of Operations IRAQI FREEDOM, ENDURING FREEDOM, NEW DAWN, and numerous worldwide contingency operations. Major Burdon holds a Bachelor of Science degree in Meteorology from Penn State University, and a Master of Arts degree in National Security Studies with a concentration in Counterterrorism from American Military University.

Abstract

Unmanned Aerial Systems (UAS) continue to play an increasing role across the spectrum of military operations. Advances in human-machine teaming, additive manufacturing, power cell density, and autonomy will position these systems to become an integral part of missions that fall inside an adversary's operational reach in the near future. At the direction of the Chief of Staff of the Air Force, the Air Command and Staff College's Airpower Vistas Research Task Force for academic year 2017 detailed the scope of anticipated threats to forward operations across defense planning scenarios through 2025. In each of these scenarios, counter-UAS (C-UAS) weapons utilizing pulsed high power microwave (HPM) energy pose a significant problem for UAS in offensive and defensive combat roles. These weapons cause electromagnetic interference (EMI) to produce effects on UAS ranging from upset to system damage. Once impractical to field due to significant power requirements, HPM weapons are now rapidly advancing in range, power, and deployability, with marked decreases in size. These advancements will enable them to be used to degrade offensive operations and neutralize forward base defense systems that utilize UAS. While hardening options for airborne systems have traditionally been prohibitively expensive and heavy for use in UAS, recent research and advances in manufacturing techniques have brought practical solutions within reach. Creating an iterative process to prioritize the application of these electronic protection measures to new and existing UAS is critical to enabling success in forward and distributed operations through 2025.

Contents

Introduction

The global power projection capability of the United States, largely unchallenged since the end of the Cold War, is increasingly in question.[1] State adversaries are rapidly developing and extending the range of anti-access/area denial (A2/AD) capabilities, while seeking inexpensive counters to exquisite US systems. Consequently, the US will likely be forced to operate within the reach of its enemies in the very near future. In this context, the execution and defense of rapid-deployable, distributed forward operations will be essential.[2] The Airpower Vistas Research Task Force (AVRTF) 2017, comprised of students from the Air War College and Air Command and Staff College, was tasked by the Chief of Staff of the Air Force with detailing the scope of these anticipated threats in 2025 to forward operations and operating locations across the Combatant Commands.[3] A product of the AVRTF, this paper asserts that while unmanned aerial systems (UAS) will play an increasing and integral role in these operations, their vulnerability to counter-UAS weapons utilizing high power microwaves (HPM) must be explored and mitigated.

Defining this unique problem set requires looking two steps ahead in the development and implementation of UAS and C-UAS technology. The capability of UAS to fill greater combat roles within an adversary's operational reach is being recognized and developed at several Department of Defense institutions, including the Air Force Research Laboratory (AFRL) and Sandia National Laboratory (SNL).[4] Advancements in automation, power cell capacity, additive manufacturing, and swarming algorithms position UAS as a formidable and highly flexible part of operations ranging from ISR to attacking air, ground and maritime targets. Counter-UAS (C-UAS) technology is also in rapid development, and includes weapons that disrupt the electromagnetic spectrum.

High power microwave weapons use intentional electromagnetic interference (EMI)[5] to disrupt, damage, or destroy electronic systems. Unlike other directed energy (DE) weapons, HPM are not attenuated greatly by atmospheric obstacles such as clouds, rain and fog. While currently expensive to develop, the cost-per-shot of these systems is relatively low. Unlike lasers, they typically have a wide aperture and are of particular use as area weapons against electronics. These characteristics make HPM systems ideal for use against UAS being utilized either individually or in swarms. C-UAS systems that use HPM have been just out of reach for decades, as the massive power requirements for such weapons have been impractical. Recent advances in this field, however, have produced capable systems that, if used in an offensive posture, can pose a threat to defensive UAS constructs. Therefore, the US cannot continue to increase the role of UAS without likewise considering their vulnerabilities to HPM weapons.

This paper uses qualitative research obtained through open and unclassified sources to advocate for improvements in hardening UAS against HPM. The first section herein will outline the current and predicted future states of UAS and HPM technology and capability through 2025. Two vignettes of future operating environments are examined in order to illustrate these predicted future states. Section II will explore principles, options, recent breakthroughs, and necessary considerations in developing countermeasures to HPM. Finally, this paper will advocate for the creation of an iterative process to prioritize the application of hardening solutions, while suggesting future research areas.

I. UAS and HPM Technology and Capabilities: Now and 2025

UAS Current State and Trends:

Identifying UAS performance gaps and vulnerabilities to HPM first requires an explanation and description of the systems to be protected, and the corresponding threat both now and projected to 2025. As UAS capabilities have rapidly evolved in recent years, so too has their categorization. Previously classed unofficially according to function and mission set, the Defense Department's 2011 release of the UAS Airspace Integration Plan assigned "Groups" to these systems based on airspeed, altitude, and weight.[6]

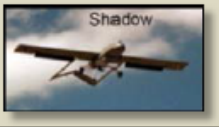
UAS Groups	Maximum Weight (lbs) (MGTOW)	Normal Operating Altitude (ft)	Speed (kts)	Representative UAS	
Group 1	0 – 20	<1200 AGL	100	Raven (RQ-11), WASP	
Group 2	21 – 55	<3500 AGL	< 250	ScanEagle	
Group 3	< 1320	< FL 180		Shadow (RQ-7B), Tier II / STUAS	
Group 4	>1320		Any Airspeed	Fire Scout (MQ-8B, RQ-8B), Predator (MQ-1A/B), Sky Warrior ERMP (MQ-1C)	
Group 5		> FL 180		Reaper (MQ-9A), Global Hawk (RQ-4), BAMS (RQ-4N)	

Figure 1: UAS Group Definitions. DoD UAS Airspace Integration Plan 2011.

Defining a current state within the UAS field is difficult, as government and private sector developers are consistently and rapidly developing new systems and upgrading the capabilities of existing platforms. In fact, the above schema classifying these systems into

Groups may already be partially obsolete, as the capabilities of small UAS are improving. For example, the most current DJI Phantom IV quadcopter is usually classified as a Group 1 UAS based on its weight and speed, but the Phantom has the altitude capability of a Group 5 UAS with a service ceiling of over 19,000 feet.[7] The pace of change of what is possible in size, weight, power, and cost (SWaP-C) suggests that altitude and speed factors should be removed from Group considerations. For the purposes of this study, however, we will use the 2011 categorization system, as it is still the accepted standard.

Unlike the connotation the popular "drone" moniker implies, current UAS have varying degrees of human interface on a spectrum from full-time remote piloted aircraft to automated systems. Full-time remotely piloted aircraft are controlled directly by line of sight, or indirectly via satellite radio and data links. Some UAS may operate in automated or partially automated roles, using pre-programmed routes and actions to lessen, or in some cases eliminate, operator requirements. Currently, these systems are regularly employed in a "single ship," or one like-aircraft environment, although actions may be coordinated within a packaged combination of manned and unmanned systems over an objective. Weapons delivery always involves direct human intervention and manual control.

The components that make up UAS are similar to those of manned aircraft systems, with the notable exception of the removal of life support, and relocation of the human operator, if one is needed, to a remote piloting location.[8] This leaves the common components of the airframe, power-plant, fuel system, sensors, communications, avionics, and electrical systems that support and integrate them. Advancements in all of these areas in the next decade can be expected.

UAS development through 2025 is likely to include substantial improvements in components and mission capability. Improvements in electronics in smaller UAS will include reduced-size, more powerful batteries capable of recharging through external means.[9] In larger systems, sensor and weapons carrying capability will continue to evolve, leading to the realization of capable platforms to augment and replace significant numbers of manned systems. Advancements in computing and algorithms will result in greater degrees of automation and autonomy for all UAS Groups. This will include the ability to swarm and cooperate with other manned and unmanned systems.

In anticipation of these innovations, AFRL began an effort to increase autonomy options of UAS in 2010, beginning with the Autonomous Control of UAS Ground Operations in the Terminal Area program.[10] Such endeavors will continue through the next decade, with the refinement of autonomous communications, navigation, collision avoidance, formation integrity,[11] ID and assessment of target intent, and target engagement.[12] Such capability, when integrated with other unmanned systems and sensors will translate well to forward offensive and defensive operations through robust situational awareness and distributed kinetic and non-kinetic effects.

Formal concepts of employment for UAS in offensive and defensive roles are still in development. However, these roles are likely to include their use in contested and denied environments where manned platforms are too few, too expensive, or too risky to use alone without augmentation from unmanned systems. Offensive roles in this context are likely to include deep strike, ISR, interdiction in denied areas, aerial resupply, direct attacks on fielded land and maritime forces, and augmenting manned platforms in offensive counter-air (OCA) operations. To defend distributed forward locations and forces, UAS will likely augment

manned platforms in defensive counter-air (DCA) operations, provide over-watch of forward forces, or as part of an integrated base perimeter defense system. However, they will likely carry increased vulnerability to electronic attack from HPM weapons due to reliance on advanced electronics.

High Power Microwaves Background, Principles, and C-UAS Applications

HPM directed energy weapons utilize energy within the electromagnetic spectrum (EMS) to disrupt, degrade, damage, or destroy targets. They can theoretically be used against all Groups of UAS. C-UAS weapons utilizing HPM are traditionally limited by power and beam physics, and can be mitigated through material hardening and redundant systems.[13] Raytheon's PHASER™ is an example of a HPM C-UAS platform, tested successfully against Group 1 and 2 UAS in 2013. Due to the low cost per shot, deep magazine, rapid advancements in power,[14] as well as the physical difficulty and cost associated hardening airborne electronics against them, HPM is positioned to become a significant threat to UAS operations through 2025.

An understanding of the current state and future potential of high power microwave systems is crucial to the development of mitigation strategies for UAS. HPM systems consist of a power source, RF wave generator, wave shaping/forming system, waveguide, antenna, and control unit.[15] They function by generating microwave radiation, and directing that energy toward the target location.[16] The ability of this energy to affect electronic equipment was first predicted and realized in conjunction with the development of radar systems from 1945 through the 1960s.[17] The weaponization of the microwave spectrum includes both continuous and pulsed wave systems. This study will concentrate on pulsed wave systems, as they may be developed specifically to create effects in the types of electronic components found in UAS.

The ability of HPM weapons to adversely affect electronics is dependent on factors inherent to the pulse generated by the weapon, target characteristics, and target distance. Factors specific to the weapon include power level, microwave frequency, pulse duration, and pulse repetition interval.[18] This pulse creates an electromagnetic (EM) field surrounding the target, typically measured in volts per meter, kilovolts per meter, or watts per square centimeter (V/m, kV/m, W/cm^2). The field produces excess energy, energy potential, or power within the target, measured in joules (J), volts (V), or amps (A). The aim is to induce a strong enough flow of electrons in the target material to cause adverse effects.[19] Field strength decreases proportional to the inverse square of target range (r), or $1/r^2$, assuming a directional antenna as the source of the pulse.

The energy that reaches the target induces effects by coupling to the component in one of two ways. "Front door" coupling occurs when energy enters the system directly through a normally utilized input device, such as an antenna. This type of coupling typically only occurs within the narrow band of the EMS that the input device was designed to receive. "Back door" coupling is the entrance of energy into the system by the field of electric potential that surrounds it. Back door coupling is more difficult to protect against, as the weapon does not need to be designed to match input device characteristics, allowing a much wider frequency band.[20] Applying these mechanisms in the context of C-UAS clarifies current and future threats to friendly systems.

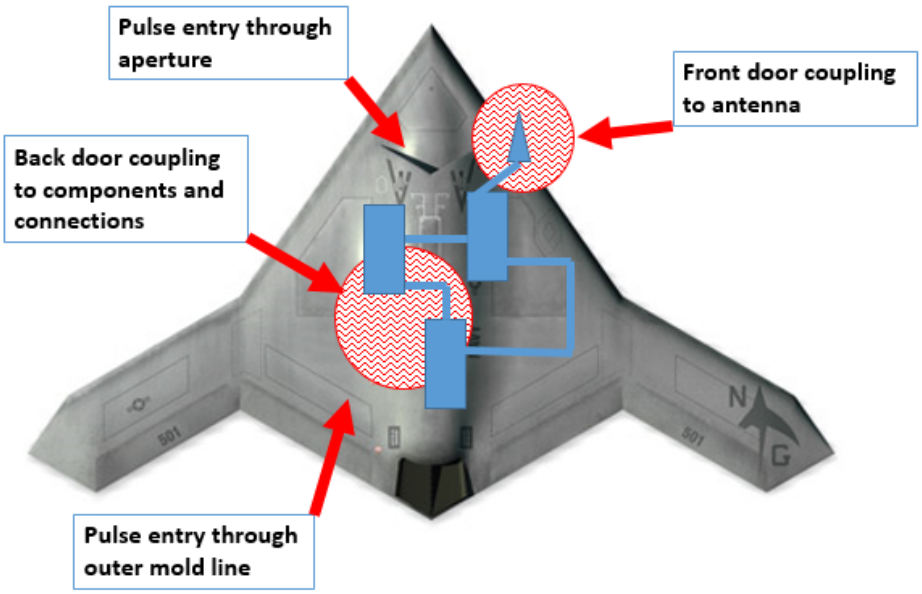


Figure 2: EMI Coupling Mechanisms

The wide variety of UAS necessitates the inclusion of myriad types of electronic components that are susceptible to HPM radiation. These include components of sensors, communications, avionics, and propulsion/power plant systems, all with unique properties and vulnerabilities. AFRL categorizes adverse HPM effects on these electronics into a five-level scale, ranging from "no effect," to "interference" (minor effect only when illuminated), "disturbance" (lingering but recoverable), "upset" (requiring intervention), and "damage" (requiring hardware, firmware, or software replacement).[21] Operational amplifiers, widely used in integrated circuits, as a common component vulnerable to upset, with a threshold of 9×10^{-10} J. Among common components most susceptible to damage are Gallium arsenide metal-semiconductor field-effect transistors (GaAs MESFET), used in radar and sensor systems, with a damage threshold as low as 10^{-7} J.[22] While upset and damage effects to common electronic components from back door coupling are typically associated with field strengths of 8 kV/m

(upset) and 15 to 20 kV/m (damage), AFRL considers a field of electrical potential of 200 V/m or stronger as a threat to sensitive electronics in general.[23] This field strength is readily attainable with current HPM systems at combat-relevant ranges.

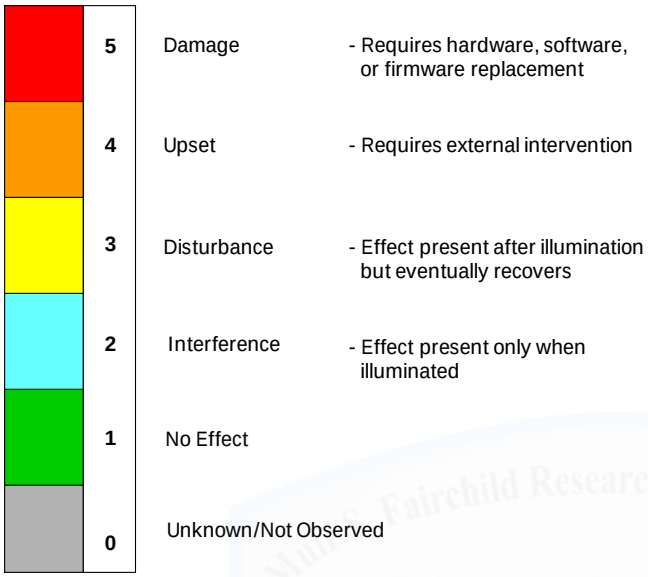


Figure 3: HPM effects on electronic components. Source: AFRL/RXCCP

Electronic Device Burnout Thresholds

Component Class	Energy (J)
GaAs MESFET	$10^{-7} – 10^{-6}$
MMIC	$7*10^{-7} – 5*10^{-6}$
Microwave diodes	$2*10^{-6} – 5*10^{-4}$
VLSI	$2*10^{-6} – 2*10^{-5}$
Bipolar transistors	$10^{-5} – 10^{-4}$
CMOS RAM	$7*10^{-5} – 10^{-4}$
MSI	$10^{-4} – 6*10^{-4}$
SSI	$6*10^{-4} – 10^{-3}$
Operational amplifiers	$2*10^{-3} – 6*10^{-3}$

Electronic Device Upset Levels

Component Type	Energy (J) @ 1 μs
Operational amplifiers	$9*10^{-10}$
TTL	$8*10^{-9}$
CMOS devices	10^{-9}
Voltage regulators	$9*10^{-8}$
Comparator	$8*10^{-9}$
VHSIC	10^{-7}

Figure 4: Electronic Device Burnout and Upset Thresholds. Source: AFRL/RXCCP

Recent advancements in HPM weapons technology have brought power requirements within the necessary parameters to cause effects in airborne electronics at realistic target distances. A 2008 Naval Postgraduate School thesis modeled HPM system capabilities based on

various combinations of the above components, ranging from easily attainable materials, to military-designed components. For example, the MATLAB-based model simulations in this thesis demonstrated that a high-end HPM system comprised of a 20 gigawatt power source operating at 2 gigahertz frequency is capable of producing 15 kV/m at a distance of 9 kilometers.[24] This is well within the capability to damage to unshielded electronics, and almost exceeds beyond visual range (BVR) thresholds, making HPM a very useful weapon against aerial targets.

The field of HPM weapons will likely continue to advance in the next decade with respect to both the US and its adversaries. Raytheon claims that during tests at Fort Sill, Oklahoma in 2013, the PHASER™ HPM was capable of upset and damage against Group 1 and 2 UAS at realistic engagement distances. The company further claims to have halved the system's size since that test, which was based on a 20 foot trailer package.[25] This type of development is by no means unique to the US. While US military funding of HPM development in 2012 was approximately $30 million, the People's Republic of China's was estimated to be in excess of $300 million per year.[26] The miniaturization, mobility, power, and range of HPM systems operated by allies and adversaries can therefore be expected to increase through 2025.

Figure 5: Raytheon PHASER™ HPM during testing at Fort Sill, Oklahoma in 2013. Source: Raytheon

Having discussed current capabilities, principles, and trends, we can now project the future use of UAS to penetrate denied environments and defend forward operating locations, as well as the threat posed to these systems from HPM. The following two vignettes illustrate the use of UAS to defend air operations in two different operating environments the US may experience circa 2025. This study will examine an attack on a robustly defended surface to air missile (SAM) battery during major combat operations, and the defense of a forward operating location (FOL). Each example exhibits a specific threat to the operation using HPM C-UAS weapons of differing size and capability.

Operational Environment Example 1: Denied Airspace Penetration in Major Combat Operations

In response to a PRC invasion of Quemoy Island, Taiwan's new administration has declared independence from the People's Republic of China, and is seeking immediate assistance and international recognition. The PRC is postured to take control of the Penghu islands before launching a massive invasion of Taiwan. As part of major combat operations to protect the

sovereignty of Taiwan, the Combined Forces Air Component Commander (CFACC) is charged with establishing localized air superiority over the eastern portion of the Strait of Taiwan.

As part of this task, flights of Group 5 UAS are launched from distributed basing in Japan's Ryuku Islands as part of a mission package to suppress and destroy the PRC's batteries of HQ-9A surface-to-air missile systems and PRC maritime assets augmenting air defenses in the Taiwan Strait. The mission calls for a combination of standoff weapons to be launched from manned platforms outside the enemy missile engagement zone, while the UAS penetrate denied airspace to overwhelm air defenses. If communications links with the UAS from base stations and manned aircraft are lost due to enemy electronic attack, the platforms are capable of continuing their mission autonomously.[27]

Figure 6: Taiwan Straits. Source: CIA World FactBook.

A flight of UAS enters the denied airspace near its target, remaining at low altitude in order to mask their approach to enemy radar. Heavy PRC jamming severs communication links,

but the flight continues to its weapons release point autonomously. Just before engaging their targets, the flight of UAS, along with the standoff weapons launched from outside the PRC missile engagement zone is hit with a pulse from a powerful HPM system at a slant range of ten kilometers. Several of the UAS experience complete electrical failure and crash, while others autonomously return to their bases with severely damaged components and firmware. The strike is unsuccessful.

The above example demonstrates the artificial intelligence being developed for "man-on the-the-loop" operation of UAS in an offensive role to penetrate denied environments. It also displays the consequences of an advanced HPM system belonging to a sophisticated state adversary. There are several nations, including the US, Russia, and the PRC, developing point defenses capable of generating such effects using HPM.[28] In contrast, the next example shows that capable HPM weapons may be used in offensive roles as well.

Operational Environment Example 2: Forward Operating Location and Hybrid War

US forces have deployed to Ämari Air Base, Estonia in response to a buildup of Russian forces along the borders of Baltic states. An ethnic Russian separatist group has been active in the nearby capital city of Tallinn, with large demonstrations and armed skirmishes with Estonian security forces in the surrounding area. As part of an integrated base perimeter defense system, Group 1 and 2 UAS are in place to provide situational awareness and maintain security for NATO forces and air assets. The larger Group 2 vehicles fly an ISR orbit at an altitude of 1,500 feet, their base-station software using advanced algorithms to identify and analyze the behavior of vehicles and personnel for signs of hostile intent.[29] The several smaller Group 1 UAS are pre-positioned in launch tubes at the base perimeter. Constructed using additive manufacturing, each

weighs less than two pounds and contains an explosive charge.[30] In the event of an attack, they are capable of swarming to overwhelm an adversary force, flying into or near hostile Groups before self-destructing after being cued by the Group 2 UAS and commanded by an operator in the base command center.[31]

Figure 7: Estonia. Source: CIA World Factbook

In early morning fog, a large group of two hundred protesters is bussed in from nearby areas and gathers at the base entrance, growing increasingly hostile to NATO security. A news van parks within 500 feet of the front gate protest, but no media crew exits the vehicle. A short time later, many of the protesters are assessed by the Group 2 UAS sensors and algorithms to be armed. Small arms fire is soon exchanged between the crowd and the main gate security forces, and authorization is given to launch a swarm of fifteen Group 1 UAS to neutralize a group of

twenty armed personnel attempting to enter the base a short distance away from the main protest group. As the swarm approaches its target, the news van, actually a portable Russian-made HPM weapon, fires a wide aperture HPM pulse, causing the entire UAS swarm to fall to the ground. With an effective range of two kilometers, the pulse also degrades and damages electronic equipment in the unshielded base command center. In the ensuing chaos, the armed group is able to access the flight line and heavily damage several aircraft before being neutralized by base security forces.[32] Russian media sources attempt to control the narrative, claiming that NATO forces have massacred a group of protesters at Ämari, who subsequently attacked and overran the base in retaliation.

This example environment exhibits the concepts of additive manufacturing, cross-cueing using UAS, swarming, and increases in battery and explosive power using nanotechnology. It also demonstrates how the SWaP-C of HPM systems can be expected to improve through 2025, likely enough to fit in a vehicle platform. Such a device could significantly degrade the defenses of a forward location, especially in the ambiguous environment of hybrid war posed by the scenario above.

II. Requirements for Electronic Protection Against HPM

The above examples show that although UAS will be of great utility in distributed combat operations, HPM weapons can threaten these assets across a wide spectrum of operating environments. In 2025, HPM systems will be smaller, more powerful, and more mobile, offering adversaries viable options to disrupt and degrade US power projection capability and operations. If UAS are to fulfill future combat roles effectively, consideration must be given to hardening

these systems against HPM. This section will explore problems inherent in addressing HPM threats, along with hardening principles and options to address these challenges.

HPM Hardening: Essential Tasks

The three challenges associated with mitigating HPM threats against airborne vehicles are pulse entry, energy induction, and architecture effects.[33] Any UAS capable of operating in an environment under threat of EA, including HPM, must address and mitigate these challenges to maintain effectiveness within its prescribed mission set. These interrelated vulnerabilities stem from the external and internal design of the vehicle. A thorough explanation of each follows.

Pulse entry is the ability of unwanted EMS energy to penetrate the target and reach vulnerable electronics. Contributing factors include outer mold line construction material and vehicle shape. In general, materials specifically designed to shield against EMI are most effective against HPM entry, followed by metallic surfaces (which conduct and attenuate the pulse), with plastics and related materials most vulnerable to penetration. Vehicle shape includes sensor apertures, vents, exhausts, and joint seams. Such openings are most vulnerable to penetration by HPM when the pulse wavelength is equal to or less than the diameter of the aperture of entry.[34]

Induction is the ability of the energy to couple via front or back door channels into the system and produce a flow of energy that exceeds upset thresholds. The vulnerability of individual components is dependent upon their material construction, function, and size. Systems of are susceptible based on the physical arrangement of individual components. This is the most

complex challenge, as combinations of these variables can have wide ranging results in induced energy when EMI is introduced.[35]

Architecture effects refer to the sum of the electronic components within the vehicle, and how their specific combination affects performance when energy is induced by EMI. A certain amount of energy induced might cause either isolated or cascading disruptions or failures, depending on the specific architecture. This threshold may be altered by changing the architecture. In general, the trend toward smaller system architecture may become a liability, as energy density within a system is higher in smaller architectures when exposed to EMI.

Hardening Options

Having identified the mechanisms by which HPM adversely effects electronics, options and methods of hardening UAS against such systems may be examined in order to develop requirements for current and future systems. The overall goals are to deny or attenuate pulse entry, while using robust electronic systems to mitigate effects within system components. The first goal may be accomplished through use of novel exterior shape in combination with negative index materials, and attenuating shielding materials.[36] The second requires the use of detection and dispersion of EMI through robust electronics architectures.

Defending against HPM pulse entry in UAS is a matter of design. Exterior shape may be used to mitigate or prevent pulse entry through seams or apertures. Negative index materials (NIM) have unique reflective and refractive properties, and may be used to disperse energy that would otherwise enter through these apertures, while allowing areas of the EMS needed by sensors to pass through. Recent NIM research has produced advances in the manipulation of the non-visible spectrum, including the redirection of microwave energy. Such materials may be

used to create aperture-less imagery sensors.[37] However, there will likely always be some penetration of energy. This problem can be alleviated through the use of shielding materials.

Building a UAS with outer mold line or internal wrap material designed to attenuate EMI may be done via two different methods. The primary option would be to incorporate shielding properties into the construction material. The 2014 DoD Electromagnetic Environmental Effects (E3) Program asserts that "Rather than relying on after-the-fact remedial measures, built-in safety by design and electromagnetic interference (EMI) mitigation techniques will be addressed in the acquisition process."[38] The cost of incorporating this protection must be considered. Since many of the principles used to harden electronics against EMP are similar to those required for HPM, there exist points of reference for related costs. Renowned physicist Lowell Wood, in a 1999 statement before the House Research and Development Subcommittee, Hearing on EMP Threats, asserted a 3-10 percent increase in modern military electronics cost if hardening is considered during acquisition.[39]

An alternative material option involves wrapping either the fuselage or internal systems in separately-developed shielding material.[40] This retrofit would be the only option for already-existing UAS designs. Such retrofits, again depending on the specific system, are traditionally expected to incur an additional cost of at least 10 percent (and in many cases much higher) of the original system expenditure using legacy shielding methods—again according to Lowell's prediction. Additionally, retrofitting any airborne system may incur performance limitations due to increased weight and aerodynamic friction. Examining EMI protection requirements for manned military aircraft can give insight into what is both required and possible for hardening unmanned systems.

EMI field attenuation (L) is measured in decibels (dB), and is ultimately expressed as a fraction (v) of original field strength. The relationship can be expressed as

$$v = 10^{-\frac{L}{20}}, \text{ or inversely, } L = 20\ log_{10}(v).$$

For example, shielding that provides 20 dB of attenuation reduces EMI field strength to 0.1 times its original value, or a reduction of 90 percent. Assuming an initial field strength at the target of 15 kV/m, the widely accepted low-end damage threshold for electronics, a vehicle would need 38 dB of shielding to attenuate the field to an acceptable level of 200 V/m. At 25 kV/m, the point at which many robust electronics are damaged, the shielding requirement becomes 42 dB of attenuation.

Most information on military aircraft shielding is close-hold in the US, partner nations, and adversaries alike. However, an interpolated value of 40-50 dB may be assumed to be a general standard across such systems, due to many militaries requiring manned airborne systems be hardened against EMP resulting from nuclear detonations. Such pulses are capable of generating field strengths in excess of 50 kV/m, which would drive a minimum attenuation requirement of 48 dB.[41] Incidentally, a 2004 study by Swedish scientists Bäckström and Lövstrand demonstrated that the 4th generation JAS-39 Gripen fighter aircraft is shielded to provide approximately 40 dB of attenuation.[42] While Groups 4 and 5 UAS operating in the NAS and in combat environments may be assumed to have between 30 and 50 dB of shielding, the shielding status of current and future Group 1-3 UAS may not have such protection requirements.

Materials used to shield UAS, whether integrated during design, or retrofitted after production, must be evaluated for cost, bulk, and weight. Incorporating conductive materials in an internal or external wrap methodology is traditionally heavy and expensive. In larger

systems, the cost of these materials is the major obstacle, while performance suffers most in smaller vehicles. These limitations may be mitigated by the use of composites, nanotechnology and new manufacturing techniques, allowing for lighter, cheaper, and more effective solutions than has been the norm. For example, US-based Conductive Composites has created a nickel-embedded non-woven material that provides from 41 to 72 dB of attenuation, depending on pulse characteristics. The material ranges from .0018 to .003 inches thick, weighs from .75 to 5.76 grams per square foot, with costs at or under $10 per square foot.[43] Another company, Glenair, has developed composite braided shielding for internal system component wrapping that is up to 80 percent lighter than traditional nickel/copper braids.[44] Such innovations would be of much use applied to UAS to prevent entry of EMI from HPM weapons.

While exterior design and shielding materials can attenuate an HPM pulse, there will always be some energy that enters the system, either through apertures or from flight in very close proximity to the HPM source. Mitigating effects of EMI once they enter UAS electronics requires a robust architecture. This may be done through a combination of detection and halting the propagation of unwanted energy. Detection requires development of microwave pulse power detectors (MPPD), while isolation and dispersion of coupled energy may be accomplished through electronic bandgaps (EBG). Exploring possibilities in each of these fields is essential in developing requirements for future UAS component architecture.

MPPD within electronic components must have a fast response time in order to detect HPM pulses before an unacceptable rise in circuit energy occurs from front or back door coupling. A 2006 University of Maryland MURI study developed MPPD using focused ion beam (FIB) manufactured Schottky diodes, as these diodes were shown to have the fastest detection times (100 nanoseconds) in relation to microwave energy.[45] The implementation of

MPPD in electronic architecture might allow the activation of physical hardware protection systems. However, more research must be done to determine adequate response times of MPPD, so that critical components can be isolated before upset or damage occurs.

The concept of EBG has been used in the manufacture of electronics to regulate energy within systems for years. Band gap engineering involves the intentional placement of EBG within systems to isolate or dissipate energy. This may be done through embedding patterns of conductive, semi-conducting, or non-conductive materials. Placement of EBG would be useful in UAS not only in printed circuit boards, but also in connective internal chassis materials that hold components in place.[46] A related option may be to isolate systems using optical switching, which would effectively isolate components from nearby sources of coupled energy.

Exterior design, material shielding, and robust internal architecture are the building blocks of UAS resiliency in a threat environment that includes HPM weapons. These solutions mitigate the problems of pulse entry, energy induction, and architecture effects through denial/attenuation, detection, and dispersion of harmful EMI. Once considered too heavy and costly to implement, advances in manufacturing and nanotechnology are bringing these building blocks within reach. However, incorporating all three solutions into every current and future UAS is not practical or fiscally responsible. Determining a way ahead requires a look at prioritizing implementation, while advocating for future research areas.

III. Recommendations: Prioritization and Future Research Areas

Using currently available technology, an ideally hardened UAS would possess four specific attributes. It would be shaped in such a manner that eliminates unnecessary apertures, while screening required apertures with negative index materials. Both the outer mold line and

internally wrapped components would be shielded in materials that provide the maximum attenuation without unacceptable losses in performance. MPPD sensors would be built into the architecture to identify microwave pulses coupling to electronic components. Finally, those components would contain optimized EBG to isolate affected components and dissipate coupled energy. Implementing every one of these solutions in every new and existing design across all five UAS Groups is not practical, nor is it fiscally responsible. Addressing the 2017 Directed Energy Professional Society Symposium, Congressman Mo Brooks, a member of the House Armed Services, Science, Space, and Technology, and Foreign Affairs Committees, emphasized that directed energy will not likely be a top DoD priority, further emphasizing the need for prioritization.[47] This section recommends a way forward in determining which UAS should be hardened against HPM, advocates future research areas, and postulates the application of this study's findings to other areas.

Prioritization Method:

Prioritizing the application of the above hardening techniques will be an iterative process. The desired product of this process should contain three elements: a list of locations and missions within an adversary's operational reach, associated UAS types threatened by C-UAS HPM weapons, and a Group order of precedence of hardening based on the concept of UAS employment and associated costs. At this time, the concept of employment for UAS in a defensive role is in its infancy, and is not well developed beyond single ship operations in offensive roles. However, the costs associated with hardening these systems are falling dramatically. Therefore, this study will use information available in early 2017 to make an

initial recommendation, with the understanding that re-examination must occur on a regular basis.

Methodology for prioritization begins with identifying adversary capability. Since the publication of the 2015 National Military Strategy, the principle focus has been on the potential adversaries of Russia, China, Iran, and North Korea, as well as violent extremist organizations (VEO). Each of these adversaries can be scrutinized as to their likelihood to develop or possess types of HPM weapons that pose a major threat to UAS through 2025, according to open and unclassified sources. Based on such predictions, this study assesses Russia and China as posing the most capable HPM threat to UAS, followed by North Korea, Iran, and VEO possessing limited capabilities through military sales and clandestine acquisition.[48]

	Point Defense	Standoff Weapons (e.g. missiles, artillery)	Vehicle Mounted, Rapid Deployable
Russia	3	3	3
China	3	3	3
North Korea	3	2	2
Iran	2	1	2
VEO	1	0	1 (with state aid)

Figure 8: Likelihood of HPM Development Through 2025. 0= Not Likely, 1=Possible, 2=Likely, 3=Highly Likely

The UAS Groups to be considered in these threat areas should be based on mission type. These can be categorized as defense of main operating bases and intermediate staging bases (MOB/ISB), forward operating bases, combat outposts and maritime vessels (FOB/COP/USN), and forward combat operations in denied environments. Given current and projected operational uses, it can be surmised that in the US inventory, Groups 1, 2 and 3 UAS are likely to make up

the largest numbers of UAS in defensive roles, with Groups 4 and 5 in offensive roles through 2025.

	Group 1	Group 2	Group 3	Group 4	Group 5
MOB/ISB			X	X	X
FOB/COP/USN	X	X	X	X	
Denied Area Access				X	X

Figure 9: Likely UAS Group Utilization Through 2025

The importance of each mission type also must be considered. For example, although there may not be many MOBs and ISBs utilizing UAS that would require shielding, missions and bases that are deemed critical to the mission of a Geographic Combatant Command (GCC) must have priority.

The final factor to weigh is cost. The price to harden UAS against HPM, while decreasing, is still significant enough at the time of this study to be given due consideration. Therefore, timely recommendations from the intelligence community will be highly important to match future enemy capabilities with hardening solutions, while considering the importance of a given mission or installation. For example, the cost of hardening Groups 1-3 is at the moment much less than Groups 4 and 5, due to system complexity and size. These small systems may also be built with additive manufacturing so as to already contain shielding materials. However, fewer numbers of higher group UAS will need to be shielded to be an effective counter to HPM. Higher performance UAS are likely to be more vulnerable primarily to traditional airborne and surface-to-air threats, and may use tactics, techniques, and procedures to avoid the engagement zones of HPM weapons. However, certain missions that require low altitude flight may require

higher levels of HPM shielding. Therefore, the highest priority should correspond to the importance of the mission or installations to be defended.

The development of counter-HPM TTP should occur both generally across all airborne electronics systems, as well as mitigation specific to individual combinations of assets and threats. Combinations of altitude, line of sight avoidance, and maneuvering so that an individual platform or swarm's exposure to EMI is minimized may have appreciable effects on HPM's ability to affect airborne systems. There are likely to be combinations of hardened and unhardened UAS operating in the future battlespace for a variety of reasons. Procedures to use these combinations effectively, given differing probabilities and degrees of exposure to HPM and intentional EMI, will minimize mission degradation.

Considering the above factors, this study asserts that the hardening of UAS and development of counter HPM TTP through 2025 should be done initially according to the following order of precedence:

Priority	Mission Set	GCC Precedence	UAS Group Order	Rationale
1	UAS in offensive roles that must access airspace denied by HPM-capable adversaries	PACOM EUCOM	Groups 4 and 5, with emphasis on hardening during procurement.	Major combat operations through 2025 are likely to require accessing and maneuvering in denied areas to achieve effects. This will simply not be possible if US platforms meant to access these environments are not hardened against HPM weapons, as PRC and Russia are developing and fielding such weapons even now.
2	UAS defending critical main operating bases (MOB) and intermediate staging bases (ISB) within adversary operational reach.	NORTHCOM PACOM EUCOM CENTCOM	Select platforms in Groups 4 and 5 required to fly at altitudes susceptible to HPM. Combined emphasis on procurement and retrofit.	Hardening the relatively small number of exquisite UAS that will protect vital installations in the US (National Capital Region and nuclear facilities/bases) and abroad provides resilience in the presence of standoff HPM weapons deployed by state actors, particularly Russia and China.
3	UAS defending US Navy Carrier and Expeditionary Strike Groups (CSG/ESG)	PACOM EUCOM CENTCOM	5,4,3,2. Emphasis on retrofitting Groups 2 and 3, and hardening Groups 4 and 5 during procurement.	The defense of CSGs is a high priority for the US Navy, as these provide essential deterrence and power projection capabilities. Surface-based or standoff HPM weapons in the maritime domain will pose a significant threat to these capabilities.
4	UAS defending forward operating locations and bases.	PACOM EUCOM CENTCOM	3, 2, 1. Emphasis on hardening during procurement.	State adversaries and VEOs enabled by them can significantly disrupt UAS ability to defend these bases in conventional and unconventional conflicts

Figure 10: UAS Hardening Priority Proposal

Again, these recommendations are a starting point. Priorities may change as information on projected adversary capability improves, or as the concept of employing UAS in defensive roles becomes part of US military strategy in a distributed basing environment.[49] Though information may change, the above method of identifying adversaries, key installations and missions at risk, the types of UAS likely to defend them, and arranging an order of precedence should comprise the basis of prioritization. If integrated into a Joint UAS Threat Working Group

(TWG), this iterative process can be used to adjust priorities as needed, creating a system that continually updates the implementation schedule of hardening solutions, while maintaining fiscal responsibility.

Future Research Areas and Other Applications:

In addition to prioritizing the hardening of UAS components, other research areas should be examined to increase these systems' ability to operate in areas subject to intentional EMI. As communications links are likely to be disrupted or denied by HPM weapons and other forms of electronic attack, alternative systems and methods may be necessary. The application of free space optical communications are a logical next step to increase UAS resiliency.

Utilizing novel areas of the EMS for communication is not an entirely new concept, but applying this area of study to UAS could allow the continued operation of a system when separated from a base station operator.[50] Formation and mission integrity could be maintained through optical communication within the area of EMI, or through contacting a platform within line of sight but outside the degraded area. Of course, the apertures for such systems would need to be protected using methods discussed previously.

The hardening solutions and recommended research areas discussed here are by no means limited to UAS. Hardening principles can be applied to vital stationary electronics, C2 structures, unmanned platforms in other domains, traditional air assets, and standoff weapons. Again, prioritizing the application of hardening and the development of counter-HPM TTP will be the key to protecting capabilities against threats in the EM spectrum.

Conclusion

The ability to rapidly combine and deploy forces, establish distributed operating locations, and execute operations across domains in contested environments comprises the backbone of US military strategic guidance through 2025. Implied tasks in this guidance includes a robust defense for these operating locations, and the ability to access denied spaces. Given the flexibility, comparatively low cost, reduction in manpower, and rapidly advancing capabilities of UAS, these systems are well positioned to become an integral part of forward operations through 2025. As the concept of using UAS in such roles is just now emerging, it is wise to think two steps ahead to ensure threats to such a construct can be mitigated.

The use of HPM as a weapon against UAS is particularly likely during this timeframe. This is due to HPM's low cost per shot, deep magazine, and recent advancements in the power systems necessary to generate EMI at combat-relevant distances. The vignettes discussed in this study reveal how HPM may be used across the spectrum of adversaries and operational environments. Understanding this threat and developing a line of effort to address our vulnerabilities to it are therefore essential tasks.

The focused research discussed here has the potential to eclipse the technical and monetary problems associated with hardening UAS against HPM. Exterior design features, material shielding, and robust electronic architecture, when combined with an iterative process of prioritized implementation, will aid in mitigating the HPM threat. Initially, hardening priorities should include UAS intended to penetrate denied areas, protecting critical installations, defending naval assets, and guarding forward operating locations. These priorities should be fulfilled through a combination of design and retrofit in order to remain cost-effective. The concepts and future research areas explored in this paper not only apply to UAS, but to the

hardening of sensitive electronics across the spectrum of multi-domain operations. Developing such practical, cost-conscious solutions ahead of anticipated threats will be an essential part of ensuring joint and coalition dominance of distributed forward operations in 2025 and beyond.

Notes

[1] I wish to thank Dr. John P. Geis, II of the Air War College, Dr. Gregory Nelson and Mr. Ben Wilson of the Air Force Research Lab, as well as the staff at AFRL, NASIC, and Sandia National Lab for their academic contributions, suggestions, and hospitality. All errors found therein are my own.

[2] *Concept for Joint Operational Access*, 17 January 2012. *Joint Concept for Entry Operations*, 7 April 2014. *Joint Concept for Rapid Aggregation,* 22 May 2015.

[3] AVRTF Memo, 2016.

[4] Site visit, 19-22 September 2016 to Air Force Research Lab, Directed Energy, Kirtland AFB, NM and Sandia National Lab, Kirtland AFB, NM.

[5] While the term EMI mostly applies to "traditional" methods of electronic warfare, as well as interference from the environment, this study will categorize HPM energy with EMI, as it is essentially the use of a particular part of the electromagnetic spectrum to cause intentional interference.

[6] UAS Task Force Airspace Integration Integrated Product Team, *Unmanned Aircraft System Airspace Integration Plan Version 2.0*, March 2011, D-2.

[7] DJI, "Phantom 4 Pro Specifications," accessed 10 March 2017, http://www.dji.com/phantom-4-pro/info#specs. Actual listed maximum service ceiling is 6,000 m (19,685 ft).

[8] International Civil Aviation Organization (ICAO), "Unmanned Aircraft Systems," *Circular 328,* 2011.

[9] David Hambling, *Swarm Troopers: How Small Drones Will Conquer the World, (*Archangel Ink, 2015), 123-137.

[10] John Keller,"Air Force looks for machine autonomy to enable UAVs and piloted aircraft to work and play well together." *Military & Aerospace Electronics,* 21, no. 8: 10, 2010. Academic Search Premier, EBSCOhost (accessed January 11, 2017).

[11] Intel, "Drones Light Up the Sky," accessed 10 Mar 2017, http://www.intel.com/content/www/us/en/technology-innovation/aerial-technology-light-show.html.

[12] Hambling, 209-242.

[13] Victor L. Granatstein et al, Institute for Research in Electronics and Applied Physics at the University of Maryland, *Effects of High Power Microwaves and Chaos in 21st Century Analog and Digital Electronics,* Final Performance Report AFOSR Grant Number F496200110374 (College Park, MD), 31 July 2006.

[14] Lt Col John P. Geis, II, "Directed Energy Weapons on the Battlefield: A New Vision for 2025," Occasional Paper No. 32, Center for Strategy and Technology at Air War College, Air University (Maxwell Air Force Base, AL), April 2003, 19.

[15] Necati Ertekin, *E-Bomb: the Key Element of the Contemporary Military-Technical Revolution*, Naval Postgraduate School (Monterrey, CA), September 2008, 16.

[16] Ibid.

[17] Doug Beason, Ph.D, *The E-bomb: How America's New Directed Energy Weapons Will Change the Way Future Wars Will Be Fought*, (Cambridge:Da Capo Press, 2005), 95-103.

[18] Eileen M. Walling, *High Power Microwaves; Strategic and Operational Implications for Warfare*, Occasional Paper No. 11, Center for Strategy and Technology at Air War College, Air University (Maxwell AFB, AL), February, 2000, 1.

[19] Site visit, 19-22 September 2016 to Air Force Research Lab, Directed Energy, Kirtland AFB, NM.

[20] Ertekin, 49.

[21] AFRL/RXCCP, See Figure 5 and Figure 6.

[22] Ibid.

[23] Ibid.

[24] Ertekin, 88. This NPS model was developed using MATLAB, however, DoD has chosen not to renew the MATLAB contract. It has been somewhat replicated in Microsoft Excel, using the Joint RF Effectiveness Model (JREM) in the interim.

[25] James Drew, "Meet Raytheon's Drone-Destroying Microwave-Energy Weapon," *Aviation Week & Space Technology,* 11 November 2016, accessed 11 January 2017, http://aviationweek.com/defense/meet-raytheon-s-drone-destroying-microwave-energy-weapon.

[26] Robert J. Katt et al, *Selected Directed Energy Research and Development for U.S. Air Force Aircraft Applications: A Workshop Summary*, (National Academies Press: Washington DC), 2013, 8.

[27] "OFFSET Envisions Swarm Capabilities for Small Urban Ground Units," DARPA Military News, 7 December 2016, accessed 8 January 2017, http://www.darpa.mil/news-events/2016-12-7.

[28] Mary Lou Robinson, "The Power of High-Powered Microwaves: Winning the Battles and Minimizing Harm," (lecture, TedX, Albuquerque, NM, 17 September 2016).

[29] UCF Crowd Behavior Algorithms article

[30] Switchblade web content, accessed 12 March 2017, https://www.avinc.com/solutions/tactical-mission-systems. The system described here might resemble an upgraded version of AeroVironment's Switchblade tactical missile system UAS.

[31] Hambling, 209-210.

[32] Ministry of Defence, "RAF Force Protection Wing Defends Camp Bastion During Taliban Attack," (United Kingdom Ministry of Defence Announcement, 19 September 2012), accessed 12 March 2017, https://www.gov.uk/government/news/raf-force-protection-wing-defends-camp-bastion-during-taliban-attack. A perimeter breach such as this, or the September 2012 attack on Camp Bastion in Helmand Province, Afghanistan, could be prevented or mitigated by the use of defensive UAS.

[33] Granatstein et al, 5.

[34] Ibid, 33.

[35] Ibid, 31.

[36] Ibid, 5.

[37] Hoai-Minh Nguyen. "Negative index materials and their applications: Recent mathematics progress," *Chinese Annals Of Mathematics 38*, no. 2: 601-628, 2017. Academic Search Premier, EBSCOhost (accessed March 1, 2017).

[38] Department of Defense Instruction (DODI) 3222.03, *DoD Electromagnetic Environmental Effects (E3) Program,* 25 August 2014, 2.

[39] Dr Lowell Wood, "Electromagnetic Pulse Threats to Civilian and Military Infrastructure," (Hearing Before the Military Research and Development Subcommittee Of the Committee On Armed Services House of Representatives One Hundred and Sixth Congress, First Session, 7 October 1999).

[40] Ben Wilson (AFRL/RXCCP), email correspondence, 10 January 2017.

[41] US Army, Test Operations Procedure (TOP) 1-2-612, *Nuclear Environment Survivability*, 15 Apr 1994, 7.

[42]Mats G. Bäckström and Karl Gunnar Lövstrand, "Susceptibility of Electronic Systems to High-Power Microwaves: Summary of Test Experience," *IEEE Transactions on Electromagnetic Compatibility*, Vol. 46 No. 3, August 2004.

[43] Conductive Composites, "Nickel Coated Non-Woven Datasheet," 2014.

[44] Glenair, "EMI/RFI Braided Shielding Solutions ArmorLite," *QuikConnect*, Vol 15 No.3, July 2011.

[45] Granatstein et al, 24.

[46] Ibid, 32.

[47] Representative Mo Brooks, (address, 2017 Directed Energy Professional Society Symposium, Huntsville, AL, 14 February 2017).

[48] Several open source materials on Russian and Chinese military developments from 2015 through 2017 mention the development of HPM weapons. Specifically, usage is purported to be in concert with existing surface to air missile systems for close-in augmentation of air defense against UAS, with ranges of up to 10 km. We can expect DPRK, Iran, and possibly VEO to eventually acquire such systems through purchase or through covert acquisition of technology. The numbers representing

likelihood for these adversaries are lower due to the uncertainty of the time it will take for this "trickle down" technology propagation to occur.

Elsa B. Kania, "The PLA's Potential Breakthrough in High-Power Microwave Weapons," *The Diplomat*, 11 March 2017, accessed 31 March 2017, http://thediplomat.com/2017/03/the-plas-potential-breakthrough-in-high-power-microwave-weapons/.

"Russia's New 'Microwave Cannon' to Disable Enemy Drones Within 10 km Radius," *Russian News Agency TASS,* 15 June 2015, accessed 31 March 2017, http://tass.com/russia/800636.

[49] Joint Concept for Rapid Aggregation 2015. UAS would be well suited to deal with the threats to distributed basing mentioned in this document's appendix.

[50] A. R. Mesleh Mansour and M. Abaza, "New challenges in wireless and free space optical communications." *Optics & Lasers In Engineering,* 89, (February 2017): 95-108. Academic Search Premier, EBSCOhost (accessed March 5, 2017).